

Hersteller, Entwicklungsorganisationen und Systemintegratoren

Entscheidungsziel: Eine nachvollziehbar begrenzte Anwendung entwickeln, deren Verhalten, Risiken, Änderungen und Übergabe technisch beherrscht werden.

Fassung 1.0 · 25. September 2026 · Adressaten: Systemarchitektur, Robotik- und KI-Entwicklung, Produktmanagement, funktionale Sicherheit, Qualität, Fertigung, Integration und technischer Service.

Dokumenttyp: strukturierte integrative Recherche mit abgeleiteten Verfahren, keine systematische Übersichtsarbeit, keine eigene empirische Robotikstudie und keine einzelfallbezogene Rechts- oder Förderberatung.

Eine unabhängige Begutachtung, Zertifizierung oder fallbezogene Rechtsberatung ist mit der Erstellung dieses Leitfadens nicht erfolgt.

Steckbrief

Merkmal	Wert
Dokumenttyp	Strukturierte integrative Recherche mit abgeleiteten Verfahren; keine systematische Übersichtsarbeit, keine unabhängige Fachbegutachtung
Zielgruppe	Systemarchitektur, Robotik- und KI-Entwicklung, Produktmanagement, funktionale Sicherheit, Qualität, Fertigung, Integration und technischer Service.
Recherche- und Rechtsstand	25. September 2026
Umfang	2.927 Wörter, 13 Seiten
Belege	0 Literatureinträge, 9 Quellenadressen
Gliederung	11 nummerierte Abschnitte, 1 Tabellen

Inhalt

1. Das richtige System als Entwicklungsgegenstand wählen	5
2. Zweckbestimmung und Einsatzkorridor operationalisieren	5
2.1 Vom Produktversprechen zur überprüfbaren Anforderung	5
2.2 Den Korridor während des Betriebs erhalten	5
3. Systemanforderungen rückverfolgbar zerlegen	5
4. Nutzfunktion und Schutzfunktion getrennt argumentieren	6
4.1 Keine Sicherheit allein aus gutem Verhalten ableiten	6
4.2 Gefährdungsanalyse nicht auf Einzeldefekte verengen	6
5. Daten und Modelle als versionierte technische Bestandteile	7
5.1 Modellidentität reicht nicht aus	7
5.2 Training, Entwicklungstest und Freigabetest trennen	7
6. Schnittstellen müssen Fehlersemantik besitzen	7
6.1 Digitale Zustände und physische Wirklichkeit zusammenhalten	7
6.2 Kommunikations- und Cloudabhängigkeiten sichtbar machen	7
7. Verifikation und Validierung als abgestimmtes Programm	8
8. Fehlerbehandlung und Wiederanlauf entwickeln	8
8.1 Fehlerklassen definieren	8
8.2 Wiederanlauf ist ein eigener Nachweis	8
9. Änderungsmanagement für Hardware, Software und Modelle	8
9.1 Jede relevante Änderung besitzt einen Wirkungsbereich	8
9.2 Sicher verteilen ist nicht dasselbe wie sicher verändern	9
10. Fertigung und Service als Entwicklungsanforderungen	9
11. Das Entwicklungs-Exit-Paket	9
Quellen zu diesem Dokument	10
Q006 · NASA	10
Q009 · Robotics Institute Germany	10
Q019 · ISO	10
Q020 · ISO	10
Q022 · NIST	10
Q023 · NIST	10
Q024 · Mitchell, M. et al.	10
Q025 · Gebru, T. et al.	11
Q032 · Europäische Kommission / DG CONNECT	11
12 Rechtliche Hinweise	12
12.1 Keine Beratung	12
12.2 Keine Zusicherung, keine Konformitätsaussage	12
12.3 Rechtsstand	12
12.4 Haftung	12

12.5 Verweise auf fremde Inhalte	12
12.6 Marken und Produktbezeichnungen	12
12.7 Urheberrecht und Nutzung	12
12.8 Keine personenbezogenen Daten	13
12.9 Unabhängigkeit	13
12.10 Anwendbares Recht	13

Impressum und Verantwortlichkeit

Die folgenden Angaben sind wörtlich dem Impressum von fluxlane.eu entnommen, abgerufen am 24. September 2026. Sie wurden nicht ergänzt und nicht umformuliert.

Angabe	Inhalt
Angaben gemäß § 5 DDG	WebTrades GmbH Am Ölberg 2 55459 Grolsheim Deutschland
Vertreten durch	Geschäftsführerin: Laurice Bussmer
Kontakt	Telefon: 0170 890 78 00 E-Mail: info@fluxlane.eu
Registereintrag	Eintragung im Handelsregister Registergericht: Amtsgericht Mainz Registernummer: HRB 54479
Umsatzsteuer-ID	Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE461650292
Redaktionell verantwortlich	Verantwortlich für den Inhalt nach § 18 Abs. 2 MStV: Laurice Bussmer, Am Ölberg 2, 55459 Grolsheim
Verbraucherstreitbeilegung	Wir sind nicht bereit oder verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Redaktioneller Hinweis des Herausgebers (wörtlich)

„fluxlane ist ein unabhängiges, redaktionelles Fachportal für Robotik, autonome physische Systeme und verkörperte KI. Der redaktionelle Geltungsbereich umfasst Industrie und Produktion, Logistik, Medizin, Pflege und Rehabilitation, Service und Haushalt sowie Forschung, Hersteller, Markt und Regulierung; künstliche Intelligenz gehört dazu, auch ohne physischen Körper. Die Inhalte dienen der allgemeinen Information und stellen keine Rechts-, Kauf- oder Anlageberatung dar. Angaben zu Preisen, Verfügbarkeit und Terminen erfolgen ohne Gewähr und können sich jederzeit ändern.“

Zitierweise

FluxLane (2026): *Hersteller, Entwicklungsorganisationen und Systemintegratoren*. Fassung 1.0, Stand 25. September 2026. Herausgegeben von der WebTrades GmbH, Grolsheim, fluxlane.eu.

Herstellung dieses Dokuments

Das vorliegende PDF ist maschinell aus der Markdown-Fassung des Leitfaden-Pakets gesetzt. Inhaltlich ist dieser Satzvorgang keine neue Sachprüfung; die zugrunde liegende Recherche- und Quellenprüfung ist im Lieferpaket dokumentiert. Setzt wurde mit IBM Plex Sans und Sora.

Abbildungsnachweis

Dieses Dokument enthält keine Abbildungen.

1. Das richtige System als Entwicklungsgegenstand wählen

Ein lernender Roboter ist nicht nur ein Modell mit einem Motoranschluss. Seine Eigenschaften entstehen aus Sensorik, Mechanik, Regelung, Modell, Werkzeug, Daten, Kommunikationswegen, Umgebung und organisatorischen Eingriffen. Eine Modellverbesserung kann wirkungslos bleiben, wenn eine mechanische Toleranz den Greifprozess begrenzt. Umgekehrt kann eine neue Kamera die Eingangsverteilung verändern und damit einen bisher gültigen Modellnachweis schwächen.

Die erste Entwicklungsaufgabe ist daher eine Systemgrenze. Sie umfasst nicht nur die Komponenten im Gehäuse, sondern alle für die bestimmungsgemäße Funktion benötigten Dienste. Wird ein Cloudsystem für Auftragsplanung, Authentifizierung oder Freigaben benötigt, gehört diese Abhängigkeit in die Systembeschreibung. Wird ein Mensch für regelmäßige Korrekturen vorausgesetzt, ist seine Aufgabe Teil des Betriebsmodells. Ein autonom genannter Hauptablauf darf solche Unterstützungen nicht aus dem System herausdefinieren.

Das RIG-Forschungsfeld Safety, Reliability and Resilience beschreibt eine Verbindung von Fähigkeitsentwicklung, Systemintegration und Nachweiserzeugung. Die hier vorgeschlagene Entwicklungslogik übersetzt diesen Gedanken in konkrete Artefakte. Sie ist eine eigene Arbeitsmethodik, kein bereits abgeschlossenes RIG-Prüfverfahren. [Q009, Assurance approach]

2. Zweckbestimmung und Einsatzkorridor operationalisieren

2.1 Vom Produktversprechen zur überprüfbaren Anforderung

Eine Anforderung muss Gegenstand, Bedingung und Akzeptanzkriterium enthalten. „Der Roboter erkennt Hindernisse zuverlässig“ ist nicht hinreichend. Erforderlich sind die relevanten Hindernisarten, Umgebungsbedingungen, Reaktionsanforderungen, Messverfahren und die Rolle dieser Erkennung in der Sicherheitsarchitektur. Die technischen Grenzwerte sind aus der konkreten Gefährdungs- und Anforderungsanalyse abzuleiten; dieser Leitfaden setzt keine universellen Geschwindigkeiten, Kräfte oder Abstände fest.

Für die Nutzfunktion werden Aufgabe, Objektverteilung, Qualitätszustand, zeitliche Anforderungen und zulässige Unterstützung beschrieben. Für die Umgebung gehören unter anderem Boden, Licht, Verschmutzung, Verkehrsorganisation, Kommunikationsqualität und räumliche Schnittstellen in den Einsatzkorridor. Die Liste ist anwendungsbezogen zu vervollständigen. Ein Luftfahrzeug, ein Laborautomat und eine mobile Transportplattform besitzen unterschiedliche Randbedingungen.

Empfohlen wird eine dreiteilige Darstellung: **zugelassen**, **noch nicht untersucht** und **ausgeschlossen**. Die mittlere Kategorie ist entscheidend. Nicht untersuchte Bedingungen dürfen weder als sichere Verwendung noch als nachgewiesene Ungeeignetheit dargestellt werden. Für jede Kategorie muss erkennbar sein, wie das System ihren Eintritt erkennt oder wie die Betriebsorganisation ihn verhindert.

2.2 Den Korridor während des Betriebs erhalten

Ein dokumentierter Einsatzkorridor nützt wenig, wenn niemand bemerkt, dass er verlassen wurde. Eine Anwendung benötigt deshalb beobachtbare Indikatoren. Beispiele sind die Identität eines Werkzeugs, ein zulässiger Layoutstand, Sensordiagnosen, definierte Netzwerkzustände oder eine validierte Eingangsdatenprüfung. Nicht jede Bedingung lässt sich automatisch überwachen. Für organisatorisch kontrollierte Bedingungen muss eine verantwortliche Rolle benannt werden.

Die Erkennung unbekannter oder ungeeigneter Eingaben ist selbst eine fehleranfällige Funktion. Eine hohe Konfidenz des KI-Modells beweist nicht, dass die Situation innerhalb des freigegebenen Korridors liegt. Deshalb ist zu prüfen, welche Annahmen mit unabhängigen technischen Mitteln abgesichert werden können und welche Restunsicherheit bleibt. Das bloße Vorhandensein eines „Unsicherheitswerts“ ist kein Ersatz für diese Prüfung.

3. Systemanforderungen rückverfolgbar zerlegen

Ein nützliches Anforderungsmodell verbindet die Ebene des Betriebsprozesses mit System- und Komponentenanforderungen. Eine übergeordnete Anforderung könnte die richtige Übergabe eines Behälters an die

richtige Station innerhalb eines Zeitfensters sein. Darunter liegen Identifikation, Navigation, Materialhandhabung, Auftragsverwaltung und Quittierung. Jede Unteranforderung benötigt einen Nachweis; zusätzlich muss geprüft werden, ob die Zusammensetzung das übergeordnete Ziel tatsächlich erfüllt.

Ebene	Beispiel einer Frage	Typischer Nachweis
Prozess	Wurde das richtige Material rechtzeitig und unbeschädigt bereitgestellt?	Ende-zu-Ende-Protokoll und unabhängige Qualitätskontrolle
System	Stimmen physischer Zustand und digitaler Auftrag überein?	Zustands- und Schnittstellentests
Subsystem	Erkennt und behandelt die Übergabefunktion ihre Fehlerzustände?	Komponenten- und Integrationstest
Modell	Welche Aufgabenvarianten beherrscht der eingefrorene Modellstand?	Getrennter Testdatensatz und repräsentative physische Versuche
Infrastruktur	Was geschieht bei unterbrochener Kommunikation?	Freigegebene Fehler- und Wiederanlauf tests

Die klassische Unterscheidung von Verifikation und Validierung ist dabei hilfreich. Verifikation prüft die Erfüllung spezifizierter Anforderungen; Validierung prüft die Eignung für den beabsichtigten Gebrauch. Ein System kann eine vollständig abgearbeitete Testliste besitzen und dennoch den falschen betrieblichen Bedarf adressieren. Die Nachweiskette muss deshalb beide Richtungen verbinden. [Q006, Verification / Validation]

Für jede Anforderung wird eine stabile Kennung vergeben. Sie verweist auf Herkunft, verantwortliche Person, Testmethode, Ergebnis, Konfiguration und zulässige Restabweichung. Ändert sich die Anforderung, muss erkennbar werden, welche Tests und Freigaben davon betroffen sind. Eine statische Tabelle ohne Versionsbezug kann diese Funktion nicht erfüllen.

4. Nutzfunktion und Schutzfunktion getrennt argumentieren

4.1 Keine Sicherheit allein aus gutem Verhalten ableiten

Ein lernendes System kann die Nutzaufgabe sehr häufig korrekt ausführen, ohne dass damit seine Sicherheit hinreichend nachgewiesen ist. Seltene Fehler können andere Folgen haben als gewöhnliche Qualitätsabweichungen. Deshalb wird jede sicherheitsrelevante Behauptung separat begründet: Welche Gefährdung wird verhindert oder begrenzt, welche Funktion übernimmt dies und auf welchen Annahmen beruht ihre Wirksamkeit?

Eine häufig sinnvolle Architektur begrenzt die Handlungsmöglichkeiten eines lernenden Systems durch gesondert abgesicherte Mechanismen. Daraus folgt aber nicht automatisch Sicherheit. Gemeinsame Sensoren, Energieversorgung, Softwarebibliotheken oder Konfigurationsfehler können die angenommene Unabhängigkeit aufheben. Auch ein korrekt ausgelöster Stopp kann in einer konkreten Anwendung neue Risiken erzeugen, etwa durch eine unzulässige Zwischenlage. Die sichere Reaktion ist deshalb anwendungsbezogen festzulegen.

Die ISO-Normenfamilien für industrielle Roboter und robotische Anwendungen unterscheiden unter anderem den Roboter vom integrierten System. In dieser Recherche wurden nur ihre Katalogangaben geprüft. Die jeweils einschlägigen Anforderungen, Prüfungen und gegebenenfalls harmonisierten Fassungen müssen von qualifizierten Personen anhand der vollständigen Normtexte und des geltenden Rechts ausgewählt werden. Eine Modellkarte oder der vorliegende Leitfaden ersetzt diese Arbeit nicht. [Q019; Q020]

4.2 Gefährdungsanalyse nicht auf Einzeldefekte verengen

Neben Komponentenfehlern sind unerwünschte Interaktionen zu untersuchen. Ein Auftrag kann doppelt ausgeführt werden, weil eine Quittierung verloren ging. Ein Roboter kann sich in einem formal zulässigen Bereich befinden, während ein Mensch eine Wartungstätigkeit ausführt, die das Leitsystem nicht kennt. Ein Modell kann ein korrekt erkanntes Objekt einer falschen Aufgabe zuordnen. Solche Fälle erfordern eine Analyse der Systemzustände und Verantwortungsübergänge, nicht nur eine Liste defekter Bauteile.

Das Gefährdungsregister beschreibt Auslöser, gefährlichen Zustand, mögliche Folge, vorhandene Maßnahmen, erforderlichen Nachweis und Restrisiko. Eine organisatorische Maßnahme wird nicht als technische Garantie

verbucht. Wenn die sichere Nutzung von einer regelmäßigen Sichtkontrolle abhängt, muss deren Durchführbarkeit, Kompetenz und Dokumentation Teil des Betriebsmodells sein.

5. Daten und Modelle als versionierte technische Bestandteile

5.1 Modellidentität reicht nicht aus

Der für einen Test relevante Stand besteht mindestens aus Modellgewichten, Architektur, Vorverarbeitung, Laufzeitumgebung, Steuerungsparametern, Sensorkalibrierung und Hardwarekonfiguration. Werden nur die Gewichte versioniert, kann dasselbe Modellkennzeichen in verschiedenen tatsächlichen Systemen laufen. Eine Freigabe sollte deshalb auf ein Konfigurationsmanifest verweisen, das die gesamte relevante Kombination identifiziert.

Bei generischen oder fremdbezogenen Modellen können Teile der Trainingshistorie unbekannt bleiben. Dieses Unkenntnis ist zu dokumentieren und durch geeignete anwendungsbezogene Nachweise zu adressieren; sie verschwindet nicht durch eine Produktbeschreibung des Lieferanten. Gleiches gilt für Lizenz- und Nutzungsgrenzen. Eine technisch verfügbare Schnittstelle begründet keine beliebige Weiterverwendung des Modells.

Modellkarten und Datensatzbeschreibungen können die Dokumentation strukturieren. Sie ersetzen jedoch weder die Prüfung tatsächlicher Leistungsgrenzen noch die Verifikation von Datenrechten. Die hier empfohlene Konfigurationsakte erweitert diese Dokumentation um physische und betriebliche Abhängigkeiten. [Q024; Q025]

5.2 Training, Entwicklungstest und Freigabetest trennen

Ein finaler Freigabetest verliert Aussagekraft, wenn die Entwicklung laufend anhand seiner Fälle angepasst wird. Die Trennung muss daher praktisch durchsetzbar sein: Datenzugriffe, Testtermine und Versionsstände werden dokumentiert. Werden bisher unbekannte Fehler aus dem finalen Test zur Verbesserung genutzt, ist dies sinnvoll, aber die nächste Freigabe benötigt einen neu definierten unabhängigen Nachweisumfang.

Die Einheit der Trennung richtet sich nach der Generalisierungsbehauptung. Bei einem Standortwechsel reicht es nicht, lediglich zufällige Einzelbilder derselben Halle in verschiedene Dateien zu verteilen. Gegebenenfalls sind ganze Standorte, Tage, Objektfamilien oder Bedienkontexte zurückzuhalten. L05 erläutert Clusterabhängigkeit, Datenleckage und statistische Unsicherheit vertieft.

6. Schnittstellen müssen Fehlersemantik besitzen

6.1 Digitale Zustände und physische Wirklichkeit zusammenhalten

Eine API, die „Auftrag angenommen“ meldet, sagt noch nicht, ob der Roboter die Aufgabe begonnen, physisch abgeschlossen oder vom Empfänger bestätigt hat. Für jede Schnittstelle ist ein Zustandsmodell erforderlich. Besonders wichtig sind Übergänge zwischen geplant, angenommen, aktiv, unterbrochen, physisch abgeschlossen, qualitätsgeprüft und endgültig verbucht.

Die Wiederholung einer Nachricht darf nicht unbemerkt eine zweite physische Aktion auslösen. Deshalb sind eindeutige Auftragskennungen, nachvollziehbare Zustandsübergänge und Regeln für Wiederholungen und Konflikte sinnvoll. Idempotenz auf Softwareebene allein garantiert jedoch keine idempotente physische Handlung. Wenn ein Greifvorgang schon stattgefunden hat, muss ein Wiederanlauf den tatsächlichen Zustand prüfen, statt blind denselben Befehl erneut zu senden.

Ein Interface Contract sollte neben Datenformaten auch Zeitverhalten, Fehlermeldungen, Zuständigkeit bei Unklarheit und Wiederanlauf regeln. Ein Timeout ist zunächst ein Informationszustand, keine Diagnose. Die sichere Reaktion kann je nach Anwendung Stoppen, Warten, Rückfrage oder ein begrenzter Ausweichablauf sein; diese Reaktion muss aus dem Schutz- und Prozesskonzept stammen.

6.2 Kommunikations- und Cloudabhängigkeiten sichtbar machen

Für jeden externen Dienst wird festgelegt, welche Funktion bei Ausfall entfällt und ob das System weiterarbeiten darf. Ein lokaler Sicherheitsmechanismus kann unabhängig von der Cloud funktionieren, während die Auftragsplanung ausfällt. Dann ist die Frage nicht nur, ob der Roboter physisch sicher bleibt, sondern auch, ob er

Material noch korrekt zuordnet und der Betreiber den Zustand versteht.

NIST SP 800-82 behandelt die besonderen Anforderungen betrieblicher Technologie, in der digitale Vorgänge physische Prozesse beeinflussen und Verfügbarkeit eine andere Rolle als in gewöhnlicher Büro-IT haben kann. Der Leitfaden nutzt diese Perspektive, ohne daraus eine bestimmte Netzarchitektur universell vorzuschreiben. [Q022, OT characteristics / architecture]

7. Verifikation und Validierung als abgestimmtes Programm

Ein technisches Prüfprogramm kombiniert unterschiedliche Nachweisarten. Komponentenprüfungen isolieren Ursachen. Integrationsprüfungen untersuchen Schnittstellen. Simulationen ermöglichen kontrollierte Variation. Repräsentative physische Tests zeigen Wechselwirkungen, die das Modell nicht vollständig erfasst. Betriebsbeobachtung ergänzt Informationen über Nutzung, Alterung und organisatorische Einflüsse. Keine dieser Methoden ersetzt alle anderen.

Vor der Durchführung stehen Anforderung, Prüfumgebung, Konfiguration, Messgrößen, Stichprobenplan und Abbruchregeln fest. Fehlerfälle dürfen nur unter den dafür freigegebenen Schutzbedingungen erzeugt werden. Ein Produktivsystem mit Personen im Gefahrenbereich ist kein allgemeiner Experimentierstand. Die Gefährdungsbeurteilung des Versuchs ist von der späteren Bewertung der Produktleistung zu unterscheiden.

Die Prüfbarkeit muss auch die Messtechnik umfassen. Wird eine Erfolgsmeldung ausschließlich aus demselben KI-System übernommen, dessen Leistung geprüft wird, kann ein gemeinsamer Irrtum unentdeckt bleiben. Für kritische Ergebnisse ist eine unabhängige Beobachtung oder geeignete Referenz sinnvoll. Ein als erledigt markierter Auftrag kann physisch falsch ausgeführt sein; ein sicherer Halt kann vom Geschäftssystem irrtümlich als technischer Totalausfall gezählt werden.

8. Fehlerbehandlung und Wiederanlauf entwickeln

8.1 Fehlerklassen definieren

Mindestens zu unterscheiden sind Qualitätsabweichungen, Nutzfunktionsausfälle, sicherheitsbedingte Unterbrechungen, Kommunikationsstörungen, Hardwaredefekte und organisatorische Blockaden. Die Klassen können sich überlagern. Das Ereignisregister sollte deshalb eine primäre Ursache, betroffene Funktionen und Folgen getrennt erfassen. Eine einzelne Zahl „Incidents“ ist ohne Taxonomie schwer interpretierbar.

Zur Fehlerbehandlung gehören Erkennen, Begrenzen, Diagnostizieren, Wiederherstellen und Überprüfen. Ein automatisch wiederholter Versuch ist noch keine erfolgreiche Recovery. Es muss feststehen, ob die ursprüngliche Aufgabe danach korrekt beendet, ein alternatives zulässiges Ergebnis erreicht oder die Aufgabe lediglich auf einen Menschen verlagert wurde. Endlosschleifen mit vielen erfolglosen Wiederholungen können eine gute momentane Autonomiequote vortäuschen, während Durchsatz und Materialqualität leiden.

8.2 Wiederanlauf ist ein eigener Nachweis

Ein Neustart kann veraltete Aufträge, unklare Objektpositionen oder ungeprüfte Werkzeugzustände übernehmen. Deshalb muss das System vor dem Wiederanlauf einen definierten konsistenten Zustand herstellen. Welche Informationen dafür erforderlich sind, hängt vom Prozess ab. Ein bloßes Zurücksetzen einer Fehlermeldung darf nicht mit der Wiederherstellung sicherer Betriebsbedingungen verwechselt werden.

Die Bedienoberfläche muss deutlich machen, was bekannt ist, was unklar bleibt und welche Handlung autorisiert ist. Eine Meldung „Fehler behoben“ darf nur auf einem tatsächlich überprüften Zustand beruhen. Mitarbeitende benötigen klare Kompetenzgrenzen: Welche Störung können sie beheben, wann muss Service hinzugezogen werden und wann bleibt die Anlage außer Betrieb? L04 übersetzt diese Anforderungen in Betreiberprozesse.

9. Änderungsmanagement für Hardware, Software und Modelle

9.1 Jede relevante Änderung besitzt einen Wirkungsbereich

Nicht jede Konfigurationsänderung benötigt dieselbe Tiefe der Prüfung. Entscheidend ist, welche Annahmen und Anforderungen sie berührt. Ein neues Werkzeug kann Nutzlast, Bewegungsraum und Wahrnehmung beeinflussen. Ein neues Modell kann bei gleicher Hardware andere Aktionen erzeugen. Ein Sicherheitsupdate kann zeitkritisches Verhalten verändern, obwohl es keine neue Nutzerfunktion bereitstellt.

Die Änderungsakte enthält Anlass, alte und neue Version, betroffene Funktionen, Gefährdungs- und Rechteprüfung, Testumfang, Freigabeberechtigung und Wiederherstellungsplan. Sie verweist auf die Nachweise, deren Gültigkeit erhalten bleibt, sowie auf diejenigen, die erneuert werden müssen. Das vermeidet zwei Extreme: ungeprüfte Updates einerseits und vollständige Neuerprobung jeder belanglosen Änderung andererseits.

9.2 Sicher verteilen ist nicht dasselbe wie sicher verändern

Authentifizierte Softwareverteilung verhindert bestimmte Manipulationen. Sie beweist nicht, dass die korrekt signierte neue Software für den Einsatz geeignet ist. Ebenso kann ein technisch erfolgreicher Rollback eine inzwischen bekannte Schwachstelle wieder einführen. Freigabe, Verteilung, Kompatibilität und Rückkehr auf einen zulässigen Stand sind deshalb getrennte Aufgaben.

NIST SSDF beschreibt Praktiken sicherer Softwareentwicklung und Schwachstellenbehandlung. Der hier empfohlene Physical-AI-Prozess ergänzt diese um die physische Konfiguration und den Einsatzkontext. Er verlangt nicht pauschal Online-Lernen oder ständige Aktualisierung, sondern die kontrollierte Behandlung jeder tatsächlich vorgesehenen Veränderung. [Q023, Practice groups]

Eine gestufte Ausrollung kann Risiken begrenzen, ist aber selbst kein Sicherheitsnachweis. Ein kleiner Testbestand muss repräsentativ genug für die beabsichtigte Änderung sein, und die Bedingungen des Tests müssen bereits zulässig sein. Eine sicherheitskritische ungeprüfte Funktion wird nicht dadurch vertretbar, dass sie zunächst nur auf einem Roboter aktiviert wird.

10. Fertigung und Service als Entwicklungsanforderungen

Ein handgebauter Prototyp kann individuelle Nachjustierungen enthalten, die in einer Serie nicht praktikabel sind. Für Produktisierung werden deshalb Stückliste, zulässige Lieferantenvarianten, Prüfmerkmale, Kalibrierung und Endprüfung benötigt. Änderungen an Komponenten müssen in derselben Konfigurationslogik erfasst werden wie Modellupdates. Ein Ersatzsensor mit gleicher Schnittstelle kann andere Messcharakteristika besitzen.

Servicefähigkeit beginnt bei Zugänglichkeit, Diagnoseinformationen, Austauschverfahren und nachvollziehbaren Zuständen nach Reparatur. Der Austausch eines Bauteils ist erst abgeschlossen, wenn die wiederhergestellte Anwendung geprüft wurde. Die genaue Tiefe dieser Prüfung hängt davon ab, welche Funktionen betroffen sind. Der Leitfaden gibt keine allgemeinen Reparaturanweisungen für gefährliche Maschinen; maßgeblich sind qualifiziert festgelegte Verfahren und Herstellerinformationen.

In der Entwicklungsplanung werden außerdem Supportdauer, Ersatzteilstadien, Datenexport und Außerbetriebnahme berücksichtigt. Eine funktionierende erste Auslieferung ist nur ein Abschnitt des Produkts. Wer mehrjährige Nutzung verspricht, benötigt die organisatorischen und technischen Mittel, um Fehler, Sicherheitsprobleme und Konfigurationsänderungen während dieser Zeit zu behandeln. Die rechtliche CRA-Einordnung und ihre zeitliche Anwendung stehen in L06. [Q032, Herstellerpflichten / Lebenszyklus]

11. Das Entwicklungs-Exit-Paket

Vor Übergabe an einen Betreiber sollten mindestens ein konsistenter Konfigurationsstand, eine klare Zweck- und Einsatzbeschreibung, nachvollziehbare Anforderungen, Prüfberichte, bekannte Grenzen, Betriebs- und Serviceinformationen sowie Rechte- und Änderungsunterlagen vorhanden sein. Der Empfänger muss unterscheiden können, welche Funktionen produktiv freigegeben, experimentell oder ausdrücklich ausgeschlossen sind.

Eine professionelle Übergabe enthält auch offene Punkte. Entscheidend ist, ob diese mit dem beantragten Nutzungskorridor vereinbar sind. Eine noch nicht validierte zusätzliche Objektklasse kann ausgeschlossen werden. Eine ungeklärte Funktion, von der die Sicherheit des vorgesehenen Betriebs abhängt, kann dagegen nicht als spätere Optimierung behandelt werden.

Prüffrage zum Abschluss: Können wir für jede wesentliche Aussage über dieses System den verantwortlichen Anforderungsstand, den passenden Nachweis, die gültige Konfiguration und die Grenzen der Übertragung benennen?

<!-- BEGIN AUTO-BIBLIOGRAPHY -->

Quellen zu diesem Dokument

Stabile Kennungen und genaue Fundstellen bleiben bei der PDF-Erstellung erhalten. Die genannten Quellen sind nicht sämtlich offline im Paket enthalten. Zugriffsgrenzen und Einschränkungen sind Teil des Nachweises.

Q006 · NASA

Systems Engineering Handbook. Stand/Publication: o. D.; Webseitenstand am Abrufdatum. Zugriff: 2026-09-25.

Original: <https://www.nasa.gov/reference/systems-engineering-handbook/> **Fundstelle:** Product Realization, Verification, Validation; Technical Management **Aussagebezug:** Unterscheidung Anforderungen, Verifikation, Validierung und Lebenszyklusmanagement. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Technische Methodenreferenz; nicht als Robotik-Rechtsnorm zu lesen.

Q009 · Robotics Institute Germany

Safety, Reliability and Resilience of AI-based Robotics. Stand/Publication: o. D.; Webseitenstand am Abrufdatum.

Zugriff: 2026-09-25. **Original:**

<https://robotics-institute-germany.de/project/safety-reliability-and-resilience-of-ai-based-robotics/> **Fundstelle:** Assurance approach / Research objectives **Aussagebezug:** Verknüpfung von Fähigkeitsentwicklung, Systemintegration und Nachweiserzeugung. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Forschungsprogramm; kein abgeschlossener normativer Prüfstandard.

Q019 · ISO

ISO 10218-1:2025 – Robotics – Safety requirements – Part 1: Industrial robots. Stand/Publication: 2025. Zugriff: 2026-09-25. **Original:** <https://www.iso.org/standard/73933.html> **Fundstelle:** Katalog: Titel, Ausgabe, Scope **Aussagebezug:** Normenfamilie für industrielle Roboter identifizieren. **Zugriff:** Katalogmetadaten und Scope eingesehen; Normvolltext nicht eingesehen **Grenze:** Nur Katalog und Anwendungsbereich geprüft; kostenpflichtiger Volltext nicht eingesehen. Keine Aussage zur aktuellen EU-Harmonisierung.

Q020 · ISO

ISO 10218-2:2025 – Robotics – Safety requirements – Part 2: Industrial robot applications and robot cells.

Stand/Publication: 2025. Zugriff: 2026-09-25. **Original:** <https://www.iso.org/standard/73934.html> **Fundstelle:** Katalog: Titel, Ausgabe, Scope **Aussagebezug:** Abgrenzung Roboterkomponente und integrierte Anwendung. **Zugriff:** Katalogmetadaten und Scope eingesehen; Normvolltext nicht eingesehen **Grenze:** Nur Katalog und Anwendungsbereich geprüft; keine klauselspezifische Normprüfung und keine Harmonisierungsaussage.

Q022 · NIST

SP 800-82 Revision 3: Guide to Operational Technology (OT) Security. Stand/Publication: September 2023. Zugriff: 2026-09-25. **Original:** <https://csrc.nist.gov/pubs/sp/800/82/r3/final> **Fundstelle:** OT characteristics; risk management; architecture and safeguards **Aussagebezug:** Verfügbarkeit, physische Prozesse und Sicherheitsanforderungen gemeinsam betrachten. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** US-amerikanische technische Empfehlung, kein unmittelbar verbindliches EU-Recht.

Q023 · NIST

SP 800-218: Secure Software Development Framework (SSDF), Version 1.1. Stand/Publication: Februar 2022.

Zugriff: 2026-09-25. **Original:** <https://csrc.nist.gov/pubs/sp/800/218/final> **Fundstelle:** Practice groups PO, PS, PW, RV **Aussagebezug:** Sichere Entwicklung, Releases und Schwachstellenbehandlung. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Bewusst feste Referenzversion; keine Behauptung, dies sei die jüngste aller Entwurfsfassungen.

Q024 · Mitchell, M. et al.

Model Cards for Model Reporting. Stand/Publication: Preprint 2018; FAT* 2019. Zugriff: 2026-09-25. **Original:** <https://arxiv.org/abs/1810.03993> **Fundstelle:** Abstract; model documentation / intended use / evaluation **Aussagebezug:** Dokumentation von Modelleigenschaften, Einsatzgrenzen und Evaluation. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Publikation schlägt Dokumentationsform vor; Karte ist kein technischer Sicherheitsnachweis.

Q025 · Gebru, T. et al.

Datasheets for Datasets. Stand/Publication: Preprint 2018; überarbeitete Publikation 2021. Zugriff: 2026-09-25. **Original:** <https://arxiv.org/abs/1803.09010> **Fundstelle:** Abstract; dataset motivation, composition, collection and uses **Aussagebezug:** Dokumentation von Datenherkunft, Zusammensetzung und vorgesehenen Verwendungen. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Dokumentierte Daten sind nicht automatisch repräsentativ, rechtmäßig oder fehlerfrei.

Q032 · Europäische Kommission / DG CONNECT

Cyber Resilience Act – Summary of the legislative text. Stand/Publication: o. D.; Webseitenstand am Abrufdatum. Zugriff: 2026-09-25. **Original:** <https://digital-strategy.ec.europa.eu/en/policies/cra-summary> **Fundstelle:** Chapter I (scope); Chapter II (manufacturer obligations); final provisions **Aussagebezug:** Produktbezug, Lebenszyklus, technische Dokumentation und Konformitätsarchitektur. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Ausnahmen und konkrete Pflichten sind am Rechtsakt und der einschlägigen Fassung zu bestimmen.

12 Rechtliche Hinweise

12.1 Keine Beratung

Diese Veröffentlichung ist ein redaktionelles Erzeugnis. Sie stellt keine Rechtsberatung, keine medizinische, pflegerische, arbeitsrechtliche oder datenschutzrechtliche Beratung und keine Beschaffungs- oder Vergabeberatung dar. Sie ersetzt insbesondere nicht die Prüfung durch Rechtsanwaltschaft, Datenschutzaufsicht, Medizinprodukteberatung, Vergabestelle, Ethikkommission nach Medizinprodukterecht oder Arbeitnehmervertretung. Wer auf Grundlage dieses Dokuments entscheidet, entscheidet auf eigene Verantwortung und hat den Sachverhalt vorher eigenständig fachlich prüfen zu lassen.

12.2 Keine Zusicherung, keine Konformitätsaussage

Die beschriebenen Verfahren, Prüfstufen und Checklisten sind redaktionelle Vorschläge. Sie sind keine Zusicherung einer Eigenschaft, kein garantiertes Ergebnis und kein Nachweis der Einhaltung einer Rechtsvorschrift. Wer ein Verfahren aus diesem Dokument anwendet, erfüllt damit keine gesetzliche Anforderung; ob eine Anforderung erfüllt ist, entscheidet die zuständige Stelle am Einzelfall.

12.3 Rechtsstand

Rechtsstände, Fristen und Fundstellen beziehen sich auf den im Dokumentkopf genannten Tag. Der KI-Rechtsrahmen wird laufend geändert; ein älterer Fristenplan darf nicht unverändert weiterverwendet werden. Genannte Gesetze und Verordnungen sind in ihrer jeweils geltenden Fassung heranzuziehen.

12.4 Haftung

Die Inhalte wurden mit Sorgfalt erstellt und, soweit im Methodenteil beschrieben, gegengeprüft. Für Richtigkeit, Vollständigkeit und Aktualität wird gleichwohl keine Gewähr übernommen. Eine Haftung des Herausgebers ist auf Vorsatz und grobe Fahrlässigkeit beschränkt; dies gilt nicht bei der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei zwingender gesetzlicher Haftung.

12.5 Verweise auf fremde Inhalte

Dieses Dokument verweist auf Inhalte Dritter, insbesondere auf Behörden-, Fachgesellschafts-, Normen- und Fachverlagsseiten. Auf deren Gestaltung und Inhalt hat der Herausgeber keinen Einfluss; für sie ist jeweils der dortige Anbieter verantwortlich. Die Adressen waren zum im Literaturverzeichnis genannten Prüfzeitpunkt erreichbar. Die Nennung eines Produkts, Herstellers oder Dienstes ist weder eine Empfehlung noch eine Bewertung seiner Eignung.

12.6 Marken und Produktbezeichnungen

Genannte Produkt-, Marken- und Unternehmensbezeichnungen sind Kennzeichen ihrer jeweiligen Inhaber und werden ausschließlich zur Beschreibung des Sachverhalts verwendet. Aus der Nennung folgt keine Verbindung zwischen dem Herausgeber und dem jeweiligen Unternehmen und keine Aussage über Zulassungs-, Konformitäts- oder Zertifizierungsstatus.

12.7 Urheberrecht und Nutzung

Dieses Dokument, sein Text, seine Tabellen und seine Abbildungen sind urheberrechtlich geschützt. Rechteinhaberin ist die WebTrades GmbH. Zulässig sind das Lesen, das Speichern und der Ausdruck für den eigenen Gebrauch sowie das Zitieren einzelner Stellen mit vollständiger Quellenangabe nach der im Impressum genannten Zitierweise. Die Vervielfältigung, Bearbeitung, Verbreitung, öffentliche Zugänglichmachung oder kommerzielle Verwertung des Dokuments oder wesentlicher Teile daraus bedarf der vorherigen schriftlichen Zustimmung der Rechteinhaberin. Das gilt ausdrücklich auch für die Übernahme von Tabellen und Abbildungen.

12.8 Keine personenbezogenen Daten

Für dieses Dokument wurden keine personenbezogenen Daten verarbeitet. Es beruht auf veröffentlichter Literatur, amtlichen Rechtsquellen und Veröffentlichungen von Fachgesellschaften; es wurden weder Beschäftigte befragt noch Patientendaten verwendet. Wer die hier beschriebenen Verfahren auf eine reale Einrichtung anwendet, verlässt diesen Rahmen: Die Auswertung von Tätigkeits-, Alarm- oder Quittierungsdaten unterliegt der Datenschutz-Grundverordnung und in der Regel der Mitbestimmung.

12.9 Unabhängigkeit

Dieses Dokument ist ohne Auftrag, ohne Finanzierung und ohne inhaltliche Beteiligung eines Herstellers, Krankenhausträgers, Kostenträgers, Verbands oder Beratungsunternehmens entstanden. Es besteht kein Vergütungs- oder Beteiligungsverhältnis zu einem der genannten Unternehmen oder Institutionen. Genannt werden Systeme, Anbieter und Dokumente, weil sie in den beschriebenen Gegenstand fallen, nicht weil sie beworben werden sollen.

12.10 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gesetzliche Verbraucherschutzvorschriften bleiben unberührt.